(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) **Offenlegungsschrift**

(10) **DE 43 44 280 A 1**

(51) Int. Cl.[6]:
H 04 L 9/32
G 06 F 11/08

(21) Aktenzeichen: P 43 44 280.3
(22) Anmeldetag: 23. 12. 93
(43) Offenlegungstag: 29. 6. 95

DE 43 44 280 A 1

(71) Anmelder:
Terzibaschian, Astrik, 13088 Berlin, DE

(74) Vertreter:
Kruspig, V., Dipl.-Ing., Pat.-Anw., 80538 München

(72) Erfinder:
Antrag auf Nichtnennung

(54) Verfahren zum Autorisieren von digitalisierten Daten aus Texten, Bildern und dergleichen

(57) Die Erfindung betrifft ein Verfahren zum Autorisieren von digitalisierten Daten aus Texten, Bildern und dergleichen sowie zum Prüfen einer derartigen Autorisation, wobei mittels des Verfahrens eine elektronische Unterschrift dokumentenabhängig erzeugt wird. Die elektronische Unterschrift wird nutzerspezifisch erstellt und kann am Ort des Empfangs der digitalisierten Daten und der in einer Zusatzdatei übertragenen elektronischen Unterschrift auf Echtheit geprüft werden. Mittels des speziellen erfindungsgemäßen Verfahrens ist es nicht nur möglich, die Unterschrift auf Echtheit zu untersuchen, sondern auch festzustellen, ob die übertragene Datei sich in dem ursprünglichen Zustand befindet oder auf dem Übertragungsweg, d. h. nachträglich, verändert wurde. Zusätzlich kann mittels des erfindungsgemäßen Verfahrens nicht nur die abzufragende Identität des Autors oder Senders eines Dokuments, sondern auch die Systemzeit, d. h. die Zeit der Erstellung der Datei, berücksichtigt werden.

DE 43 44 280 A 1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

BUNDESDRUCKEREI 05. 95 508 026/265

Beschreibung

Die Erfindung betrifft ein Verfahren zum Autorisieren von digitalisierten Daten aus Texten, Bilden und dergleichen gemäß dem Patentanspruch 1.

Bei der Entwicklung von Mikrocomputern oder anderen auf Mikroprozessoren basierenden Baugruppen spielt die Systemsoftware und der Zugriffsschutz auf eine derartige Software eine besondere Rolle. Zum Schutz der Software gegen unberechtigtes Kopieren, Verändern oder Zerstören kann mit einer speziellen Hardware, nämlich einem sog. Schlüssel-EPROM ein Zugriffsschutz realisiert werden. Hierfür befindet sich zusätzlich zur Speichermatrix eines Standard-EPROM ein weiterer EPROM zum Softwareschutz. Nach Aktivieren eines Schutzmechanismus wird der Inhalt des Speichers erst nach dem erfolgreichen Abschluß einer Authentisierungssequenz freigegeben. Gesteuert durch einen Mikroprozessor überprüfen sich mindestens zwei spezielle EPROM's gegenseitig. Ein derartiges Verfahren im Handshake-Betrieb greift z. B. auf die Überprüfung einer 64 Bit langen Schlüsselzahl zurück, die identisch in beide EPROM's einprogrammiert wurde. Der Schlüssel selbst ist, nachdem der Systemschutz einmal programmiert worden ist, weder im ab- noch im aufgeschlossenen Zustand lesbar. Um die Schlüsselzahlen vergleichen zu können, müssen diese über einen internen Datenbus zwischen den Eproms transportiert werden. Damit die Geheimzahl auf dem Bus nicht unberechtigt gelesen werden kann, wird diese nur verschlüsselt übertragen.

Mit dem vorstehend genannten Beispiel kann zwar die intern in einem Eprom abgelegte spezielle Betriebssoftware vor unberechtigtem Zugriff oder Kopieren geschützt werden, jedoch kann nicht festgestellt werden, ob die Software von einem hierzu berechtigten, der z. B. den Schlüssel zum Eingeben oder Auslesen kennt, verändert bzw. verifiziert wurde.

Auch im elektronischen Rechtsverkehr hat es sich herausgestellt, daß eine Manipulation an übertragenen digitalisierten Daten ohne Kontrolle, ob eine derartige Datenveränderung stattgefunden hat, möglich ist. Dies ist bezüglich der Rechtsverbindlichkeit bestimmter über elektronische Datenüberstragungsstrecken ausgetauschter Dateien, wie z. B. Vertragstexten, von außerordentlichem Nachteil. Weiterhin problematisch ist die Tatsache, daß die Rechtsverbindlichkeit bestimmter Handlungen an das Formerfordernis der Unterschrift gebunden ist. Hieraus entsteht also ein Widerspruch zwischen der eindeutigen technischen Effizienzsteigerung durch den elektronischen Rechtsverkehr an sich und dem Problem der Formerfordernis der Unterschrift im klassischen Sinne.

Es ist daher Aufgabe der Erfindung, ein Verfahren zum Autorisieren von digitalisierten oder digitalisiert vorliegenden Daten aus z. B. Texten, Bildern und dergleichen anzugeben, wobei gleichzeitig nach der Übertragung der entsprechenden Daten bzw. Dateien über Datenträger oder Datennetze beim Empfänger nachgeprüft werden kann, ob die entsprechende Datei rechtmäßig autorisiert wurde und/oder ob die Datei unverändert geblieben ist. Unter dieser speziellen Prüfung soll verstanden werden, daß mit einer außerordentlich geringen Irrtumswahrscheinlichkeit festgestellt werden kann, ob ein Dokument so, wie es empfangen wurde, auch tatsächlich mit dem Dokument oder der Datei übereinstimmt, die vom Autor ursprünglich ausgefertigt und versandt wurde.

Der Grundgedanke der Erfindung besteht darin, eine Strategie für ein offenes Autorisierungs- und Prüf- oder Kontrollsystem vorzustellen, wobei alle Teilnehmer im System gleichberechtigt sind und sowohl autorisieren als auch die Autorisation von Dateien testen können. Das System ist derart ausgestaltet, daß jederzeit neue Teilnehmer in den elektronischen Austausch der Daten aufgenommen werden können. Des weiteren besteht ein wesentlicher Gedanke der Erfindung darin, daß die übertragenen Daten bzw. Dokumente am Empfangsort auch lesbar sind, wenn der betreffende Empfänger nicht Nutzer des eigentlichen Systems ist, also die Autorisierung weder prüfen will noch prüfen kann.

Die Texte, Bilder oder anderen Informationen werden also nicht zum Zweck der Verschlüsselung, sondern nur zum Zweck der Übertragung digitalisiert. Es wird also keine Verschlüsselung der Daten selbst vorgenommen.

Mittels der Erfindung ist es möglich, eine elektronische Unterschrift zu erstellen, wobei diese Unterschrift senderseitig ausgefertigt und empfängerseitig auf Echtheit geprüft werden kann.

Hierfür wird aus allen Zeichen einer Ausgangs- oder Ursprungsdatei eine textabhängigen Unterschrift erzeugt, die aus einer bestimmten Anzahl von Zeichen, die in eine Zusatzdatei einfließen, besteht. Im einfachsten Fall besteht die Zusatzdatei aus einer Prüfsumme aus den Zeichen der Ursprungsdatei. Zusätzlich wird die Identität des Autors bzw. des Nutzers bei der Bildung der textabhängigen Unterschrift implementiert. Dies geschieht beispielsweise dadurch, daß der Nutzer die vorerwähnte Prüfsumme in definierter Weise verändert oder verschlüsselt.

Der Empfänger der Datei wird unter Nutzung des erfindungsgemäßen Verfahrens in die Lage versetzt, zum einen den Zustand der Datei und zum anderen die Identität des Autors zu bestimmen bzw. wiederzuerkennen. Des weiteren ermöglicht das erfindungsgemäße Verfahren eine Sicherheit gegen unberechtigtes Verändern oder Autorisieren, ohne daß ein im System eingebundener Empfänger dies bemerkt.

Die textabhängige Unterschrift wird unter Verwendung eines Codierwortes erstellt; dies kann z. B. durch eine Verschlüsselung der vorerwähnten Dateiprüfsumme mit diesem Codierwort erfolgen. Die erstellte textabhängige Unterschrift besteht aus einer endlichen Anzahl von Zeichen, die dem Empfänger, wie dargelegt zweckmäßigerweise in einer Zusatzdatei, mitgeteilt werden. Der Empfänger bildet dann am Empfangsort noch einmal die textabhängige Unterschrift nach und vergleicht diese mit der übermittelten. Um eine hohe Fälschungssicherheit zu erreichen, wird erfindungsgemäß das Codierwort nicht offen übertragen. Zusätzliche Sicherheit ist dadurch gegeben, daß das Codierwort Identitätsmerkmale des Autors bzw. Nutzers enthält.

Erfindungsgemäß ist das Codierwort variabel und wird vom Autor bzw. Nutzer senderseitig erzeugt. Um empfängerseitig prüfen zu können, wie der Autor, d. h. der Sender, sein Codierwort gebildet hat, verfügen alle Nutzer des Systems über einen Codierschrittalgorithmus, welcher geheim ist und der das Codierwort bilden kann. Die Bildung des Codierwortes geschieht zweckmäßigerweise mittels Hardware intern, so daß der eigentliche Nutzer des Systems das Codierwort selbst nicht erfährt.

Da die Codierschritte für alle Nutzer des Systems im wesentlichen identisch sind, wird erfindungsgemäß einer oder mehrere der Codierschritte mit einer Serien-

nummer individualisiert. Jeder Nutzer kennt dabei nur die Seriennummer der eigenen Codierschritte. Wenn dann ein weiterer Codierschritt das Codierwort unter Verwendung der spezifischen Seriennummer erzeugt, steckt in der dann hieraus entstandenen textabhängigen Unterschrift ein Merkmal, das die Originalität bzw. die Identitätsmerkmale des Autors kennzeichnet.

In der eingangs erwähnten Zusatzdatei wird die Serien- bzw. Kennummer mitübertragen, so daß der Empfänger in die Lage versetzt wird, die senderseitige Prozedur nachzuvollziehen. Grundsätzlich benutzen die Codierschritte beim Erzeugen der textabhängigen Unterschrift die spezifischen eigenen Seriennummern, d. h. beim Überprüfen einer Unterschrift empfangsseitig die mitgeteilte Seriennummer der Senderseite bzw. des Autors.

Um einen Zugriffsschutz auf eigene Codierschritte zu erreichen, wird mit einem weiteren speziellen Codierschritt jeder Seriennummer mathematisch eindeutig ein Paßwort zugeordnet. Da die Seriennummern jeweils individualisiert sind, sind es die Paßwörter auch. Bleibt das Paßwort außer für den jeweiligen Benutzer, d. h. Sender, allen anderen Nutzern, d. h. Empfängern, gegenüber geheim, wird das Paßwort zu einem Zugriffsschutz für die eigenen Codierschritte.

Zusätzlich kann zur weiteren Erhöhung der Sicherheit der Autorisation bei der Bildung des Codierwortes die offene Seriennummer und das geheime Paßwort des jeweiligen Senders verwendet werden.

Erfindungsgemäß besitzt also jeder Systemnutzer erste Codierschritte, die aus einer Kennung bzw. Seriennummer in der Lage sind, ein Paßwort in eindeutiger Weise abzuleiten. Des weiteren besitzt jeder Nutzer zweite Codierschritte, die aus dem Paßwort und der Seriennummer des Nutzers in eindeutiger Weise ein Codierwort ableiten, welches aus einer bestimmten Anzahl von Zeichen besteht. Beim Autorisieren benutzt der Nutzer zwangsläufig die eigene Seriennummer und das eigene Paßwort. Beim Prüfen einer Unterschrift wird dann nur die übermittelte, fremde Seriennummer eingegeben und das Paßwort unter Verwendung der ersten Codierschritte intern rekonstruiert, ohne daß es nach außen, z. B. über einen Monitor, gegeben wird bzw. sichtbar ist.

Dritte Codierschritte, die jedem Nutzer zur Verfügung stehen, bilden unter Verwendung des Codierwortes aus allen Zeichen der zu autorisierenden Ursprungsdatei in eindeutiger Weise die erwähnte textabhängige Unterschrift, die ebenfalls aus einer bestimmten Anzahl von Zeichen besteht.

Das erfindungsgemäße Verfahren soll nunmehr anhand eines Ausführungsbeispiels näher erläutert werden.

Um eine Datei zu autorisieren, wird zunächst durch Eingabe bzw. Übergabe des Paßwortes der Vorgang gestartet. Dann wird mittels einer Seriennummer und unter Zuhilfenahme von ersten Codierschritten ein internes Kontrollpaßwort gebildet. Nach Prüfung der Übereinstimmung des eingegebenen und intern erstellten Paßwortes ist die Berechtigung zur Autorisation überprüft und akzeptiert. Nun wird mittels der zweiten Codierschritte das Codierwort gebildet und das gebildete Codierwort den dritten Codierschritten zugeführt. Diese erzeugen dann aus der Ursprungsdatei die textabhängige Unterschrift.

Das erfindungsgemäße Verfahren wird zweckmäßigerweise mittels eines Personal Computers realisiert, welcher über zusätzliche Hardware-Steckeinheiten verfügt, die die erwähnten Codierschritte in entsprechend geschützter und gesicherter Form aufweisen. Ein externer Eingriff oder ein Auslesen der Codierschritte ist nicht möglich.

Die Steuerung der Eingaben, Ausgaben und Abfragen erfolgt durch eine entsprechend gestaltete Benutzeroberfläche. Die Benutzeroberfläche legt die Seriennummer und die textabhängige Unterschrift in einer Zusatzdatei ab, die dann die erwähnte Unterschrift enthält.

Die ursprüngliche Datei kann in bekannter Weise und unverändert mittels eines Wortprozessors gelesen oder auch verändert werden.

Aufgrund einer mathematischen Eindeutigkeit der zweckmäßigerweise in der Hardware abgelegten Codierschritte ist eine vollständige Reproduzierbarkeit der Ergebnisse bei jedem lokalen Nutzer des erfindungsgemäßen Systems erreichbar.

Der Empfänger einer Datei übergibt zunächst die in der Zusatzdatei bzw. elektronischen Unterschrift enthaltene Seriennummer an einen empfängerseitig vorgesehenen Hardware-Komplex, der die ersten Codierschritte aufweist, um daraus das Paßwort des Autors wiederherzustellen.

Diese Wiederherstellung erfolgt aber nicht nach außen sichtbar, sondern nur intern und wird an ebenfalls empfängerseitig vorhandene zweite Codierschritte weitergegeben. Die zweiten Codierschritte erzeugen dann das Codierwort unter Nutzung der dritten Codierschritte. Dann wird aus dem intern empfängerseitig erstellten Codierwort und der Ursprungsdatei noch einmal die textabhängige Unterschrift nachgebildet, nicht nach außen gegeben und intern mit der übertragenen, textabhängigen Unterschrift verglichen.

Stimmt beides überein, so wird die Unversehrtheit der Datei bzw. die Rechtmäßigkeit der Autorisation festgestellt. Der besondere Vorteil der Erfindung liegt darin, daß eine Fälschung nur dann möglich ist, wenn man gleichzeitig Paßwort und Seriennummer des Autors kennen würde, und gleichzeitig alle erwähnten Codierschritte beherrscht. Da jeder zweite Codierschritt am Ort jedes Systemnutzers nur das eigene Paßwort abfragt, müßte man also um Fälschungen vornehmen zu können, die zweiten Codierschritte des Autors bzw. Senders und dessen Paßwort kennen und benutzen. Aufgrund der Tatsache, daß in der elektronischen Unterschrift durch die zweiten Codierschritte die Individualität der Datei und des Autors gegeben ist, kann ein anderer Autor auch bei einer identischen Datei nur eine andere elektronische Unterschrift produzieren. Die erwähnte bekannte Serien- oder Kennummer dient nur dazu, das geheimzuhaltende Paßwort zwischen den Nutzern auszutauschen, ohne daß das Paßwort den Nutzern selbst gegenseitig bekannt wird. Mittels der lokal überall vorhandenen und identischen ersten Codierschritte wird lediglich intern das Paßwort wiederhergestellt, aber nicht nach außen erkennbar ausgegeben.

In einer Ausgestaltung der Erfindung ist es zusätzlich möglich, die in vielen Betriebssystemen mit einer Datei verknüpfte Systemzeit beim Codieren der textabhängigen Unterschrift miteinzubeziehen. Hierdurch könnte ein Dokument sowohl hinsichtlich seines Autors als auch der ursprünglichen Entstehungszeit geprüft werden.

Das erfindungsgemäße Verfahren soll abschließend und zusammenfassend anhand des nachstehenden Ablaufbeispiels erläutert werden.

Ablaufbeispiel

1. Start des Autorisierungs-Verifikationsprogramms;
2. Frage, ob autorisiert oder verifiziert werden soll.

Wenn Autorisierung:

3a Paßwort abfragen;

4a Aus der Seriennummer das interne Paßwort erzeugen und mit dem Eingegebenen vergleichen. Bei Nichtübereinstimmung Abbruch des Vorgangs, sonst weiterer Ablauf mit einem einfachen Algorithmus, der darin besteht, den Ziffern der Seriennummer die Entsprechung des ASCII-Zeichensatzes zuzuordnen;

5a Abfrage des Dateinamens der Datei, die autorisiert werden soll;

6a Öffnen der Datei und zeichenweises Einlesen der gesamten Datei. Jedes Zeichen wird als 8-Bit-Zahl gedeutet und mit der eigenen Seriennummer multipliziert. Vom Produkt werden die unteren 8 Bit verwendet und aufsummiert. Von der gebildeten Summe werden wieder die unteren 8 Bit als textabhängige Unterschrift abgetrennt;

7a Öffnen einer neuen Datei mit dem angegebenen Dateinamen und der Endung "sig.";

In diese Datei wird die eigene Seriennummer und die textabhängige Unterschrift geschrieben. Schließen beider Dateien.

Wenn Verifikation:

3b Dateinamen abfragen;

4b Prüfen, ob Datei mit angegebenem Dateinamen und Endung .sig existiert. Wenn nicht, Fehlermeldung. Wenn ja, Öffnen der Datei Name .sig und Einlesen von Seriennummer und textabhängiger Unterschrift.,

5b Starten analog Schritt 6a, allerdings unter Verwendung der in Name .sig enthaltenen Seriennummer;

6b Vergleich des Ergebnisses von Schritt 6a mit der textabhängigen Unterschrift aus Name .sig. Wenn beides übereinstimmt, Ausgabe "Autorisierung in Ordnung", sonst "Autorisierung nicht in Ordnung".

Die Erfindung ist zum einen beim elektronischen Austausch von digitalen Dateien in Computersystemen und in Computernetzwerken, aber auch bei der Übermittlung von Nachrichten mittels drahtloser digitaler Übertragung oder Telefaxsystemen anwendbar. Die Codierschritte bzw. die Kernroutinen sind zweckmäßigerweise in einem oder mehreren Spezialschaltkreisen einer Hardwarebaugruppe realisiert. Das notwendige Hardware-Paßwort für die zweiten Codierschritte kann auch als eine Art körperlicher Schlüssel realisiert werden.

Aufgrund der extremen Fälschungssicherheit erfüllt die mit dem erfindungsgemäßen Verfahren ausführbare elektronische Unterschrift wesentliche Erfordernisse, so daß von einer Rechtsverbindlichkeit von Handlungen, die mit einer derartigen Unterschrift bestätigt wurde, ausgegangen werden kann.

Patentanspruch

Verfahren zum Autorisieren von digitalisierten Daten aus Texten, Bildern und dgl. sowie zum Prüfen einer derartigen Autorisation mit folgenden Schritten:

— Eingabe eines benutzerspezifischen Paßwortes am Ort der Autorisation bzw. der Erstellung einer oder mehrerer Dateien aus den digitalisierten Daten, wobei mittels erster Codierschritte aus einer Serien- oder Kennummer ein internes Paßkontrollwort erstellt wird und nach positiver Vergleichsprüfung zwischen dem internen Paßkontrollwort und dem eingegebenen benutzerspezifischen Paßwort mittels zweiter Codierschritte ein internes Codewort gebildet wird;

— Festlegen einer Prüfsumme bzw. einer Daten- oder Dateiverschlüsselung mit Hilfe dritter, durch das interne Codewort determinierter Codierschritte, wobei die Dateiverschlüsselung derart erfolgt, daß mit einer Änderung einer kleinsten Dateieinheit bzw. der kleinsten auflösbaren bzw. übertragenen Datenmenge eine neue spezifische Dateiverschlüsselung gebildet wird;

— Ausgabe bzw. Senden der Dateiverschlüsselung einschließlich der Serien- oder Kennnummer in Form einer Zusatzdatei, die gemeinsam mit den Ausgangsdaten übertragen wird und die die Funktion einer elektronischen Unterschrift erfüllt;

— Eingabe bzw. Empfang der Zusatzdatei, wobei die hierin enthaltene Serien- oder Kennnummer mittels empfangsseitiger erster Codierschritte, die den ersten senderseitigen Codierschritten entsprechen, das Paßwort des Senders bzw. des senderseitigen Nutzers intern rekonstruiert wird, aus dem Paßwort mittels empfangsseitiger zweiter Codierschritte, die den senderseitigen zweiten Codierschritten entsprechen, intern das Codierwort gebildet und mit Hilfe dritter empfangsseitiger Codierschritte und den Ausgangsdaten bzw. der Ausgangsdatei eine Kontrollverschlüsselung erfolgt und intern die elektronische Unterschrift empfangsseitig erzeugt wird,

— Vergleichen der intern empfangsseitig erzeugten elektronischen Unterschrift mit der senderseitig übertragenen elektronischen Unterschrift und nach positiver Vergleichsprüfung Bestätigung der Echtheit der elektronischen Unterschrift bzw. des unveränderten oder unversehrten Zustands der Ausgangsdaten bzw. Ausgangsdatei.